Obfuscation to Thwart Un-Trusted Hardware

NOTE: The Solicitations and topics listed on this site are copies from the various SBIR agency solicitations and are not necessarily the latest and most up-to-date. For this reason, you should use the agency link listed below which will take you directly to the appropriate agency server where you can read the official version of this solicitation and download the appropriate forms and rules.

The official link for this solicitation is: http://www.acq.osd.mil/osbp/sbir/solicitations/index.shtml

Agency:
Department of Defense

Release Date:
November 20, 2013
Branch:
Office of the Secretary of Defense

Open Date:
November 20, 2013
Program / Phase / Year:
SBIR / Phase I / 2014

Application Due Date:
January 22, 2014

Solicitation:
2014.1

Close Date:
January 22, 2014
Topic Number:
OSD14.1-IA1

Description:
OBJECTIVE: To develop innovative methods for mutating or obfuscating the processes of network security appliances or tactical communication systems. To make the path of the processes and data through hardware non deterministic, thereby thwarting any supply chain attacks that rely on the deterministic nature of computing to exfiltrate data and compromise operations. To mask the data and processes such that information exfiltrated from compromised hardware is not useful to an adversary. DESCRIPTION: With more and more of the hardware that the U.S. Army relies on for critical communications and security being manufactured in whole or in part in countries not sympathetic to the goals of this Nation, supply chain tampering is of a greater and greater concern. Tampering with components as they are produced can have catastrophic effect. From a security perspective, the possibility of supply chain attacks undermines the trust that can be placed on a system. Supply chain attacks can involve the insertion of hardware modules or embedded code into hardware devices. These insertions can exfiltrate data or allow backdoor access into systems by the parties responsible for their insertion. Detecting these insertions is costly and difficult, especially with many components coming from many places; all of which could have any of these types of insertions. These inserted modules rely on the user being unaware of their presence, and performing tasks in a predictable manner. The aspect of a predictable manner is very important to the developers of the supply chain attacks. In the case of network security appliances, the hardware"s intended use is known at the time of manufacture, and its use can easily be predicted. In many cases the behavior of the software is very well known, and its path through the hardware can easily be predicted. This can give the adversary easy access to usernames, passwords, and data that should be encrypted. It can also provide the adversary with the means to stealthily bypass the

security features on the system. If network security appliance or tactical communication system processes and data can be masked or modified in such a way that if exfiltrated it is no longer useful, or even harmful, to the adversary it will restore trust to the system. If the processes can be rerouted through the hardware, such that its path is unpredictable, these malicious insertions would no longer be able to reliably exfiltrate useful data, or attack processes. Developing a means of restoring trust by the software architecture is a novel idea. It will lead to a more secure computing environment, because we will be able to place more trust in the systems. It will also prevent the cost of construction and operating new and trusted computer components manufacturing facilities, or embedding inspectors at factories around the world. PHASE I: Define software architecture that would be compatible with network appliance and/or tactical communication hardware that would enable security applications or tactical communication systems to operate in a trusted manner on hardware assumed to be untrusted. Describe and develop creative methods, techniques, and tools that would allow for the implementation of such an architecture. PHASE II: Develop, implement and validate a prototype system that utilizes the architecture, tools, and methods from Phase I. The prototypes should be sufficiently detailed to evaluate scalability, usability, and resistance to malicious attack. Efficiency is also an issue that should be explored, although it is less critical than overall scalability. PHASE III DUAL USE APPLICATIONS: The increasingly global market for computer hardware will continue to put the production of hardware in places not sympathetic to the United States Military or commercial sector. This application will have a broad market in the commercial sector as well where the protection of intellectual property is becoming increasingly difficult.